

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,)	No. CR16-5110RJB
)	
Plaintiff,)	SECOND MOTION AND
)	MEMORANDUM IN SUPPORT OF
v.)	MOTION TO COMPEL
)	DISCOVERY
)	
DAVID TIPPENS,)	<i>[Oral Argument Requested]</i>
)	
Defendant.)	NOTED: December 16, 2016

UNITED STATES OF AMERICA,)	No. CR15-387RJB
)	
Plaintiff,)	SECOND MOTION AND
)	MEMORANDUM IN SUPPORT OF
v.)	MOTION TO COMPEL
)	DISCOVERY
)	
GERALD LESAN,)	<i>[Oral Argument Requested]</i>
)	
Defendant.)	NOTED: December 16, 2016

UNITED STATES OF AMERICA,)	No. CR15-274RJB
)	
Plaintiff,)	SECOND MOTION AND
)	MEMORANDUM IN SUPPORT OF
v.)	MOTION TO COMPEL
)	DISCOVERY
)	
BRUCE LORENTE,)	<i>[Oral Argument Requested]</i>
)	
Defendant.)	NOTED: December 16, 2016

I. INTRODUCTION

Defendants David Tippens, Gerald Lesan and Bruce Lorente, through their attorneys, respectfully move the Court pursuant to Fed. R. Crim. P. 16(c) and (d) for an Order compelling discovery of information related to the recent publication of NIT code that, based on the available information, appears to be Operation Pacifier code that the Government has refused to provide to the defense.

The trials are now scheduled for January 23, 2017, with a pretrial motion deadline of December 16, 2016.

II. FACTS AND ARGUMENT

The Government maintains that the NIT code is secret and has invoked provisions of the Classified Information Procedures Act to justify nondisclosure of the code to the defendants.

On or about November 29, 2016, NIT code was sent from an unknown source to Mozilla (producer of the Tor browser). Mozilla has released a “patch” for the browser vulnerability that the NIT used to bypass or alter computer security settings and gain access to target computers. Eduard Kovack, *Mozilla Patches Firefox Zero-Day Exploited to Unmask Tor Users*, Security Week, Dec. 1, 2016 (“Security updates released on Wednesday for Firefox and the Tor Browser address a zero-day vulnerability exploited to deanonymize Tor users. Evidence suggests that the exploit may have been used by a law enforcement agency in an operation targeting child pornography distributors.”);¹ BBC.com, *Spyware Tracks Child Sex Abuse Site Users*, Dec. 1, 2016.² According to one expert, the NIT may utilize a “memory corruption

¹ Available at: <http://www.securityweek.com/mozilla-patches-firefox-zero-day-exploited-unmask-tor-users>

² Available at: <http://www.bbc.com/news/technology-38170563>

1 vulnerability” that can result in the alteration or deletion of data stored on infected
2 computers.

3 Given the limited information that is publicly available, defense experts are
4 presently unable to determine whether the NIT code obtained by Mozilla is in fact the
5 Operation Pacifier code. However, they have advised counsel that there is good cause to
6 believe that it is the same or similar code.

7 Equally importantly, even if the codes are not identical, defense experts believe
8 that the vulnerability that the FBI relied on for Operation Pacifier may have been
9 neutralized. In that case the Operation Pacifier NIT is no longer viable and
10 Government’s interest in not disclosing the code would be substantially reduced or
11 eliminated.

12 On December 1, defense counsel asked the Government to confirm or deny
13 whether the code obtained by Mozilla and its security patch are related to the Operation
14 Pacifier code. The Government has declined to answer this inquiry.

15 According to various news sources, the NIT code obtained by Mozilla may have
16 been developed by a private contractor that works closely with federal law enforcement
17 and national security agencies. There are also reports that the contractor may have sold
18 the code to a private client or foreign government, or that it was captured by a third
19 party during the unencrypted portions of the Operation Pacifier NIT transmissions.

20 News sources have also reported that the NIT code had circulated for some time
21 prior to Mozilla’s release of a security patch. If that is true, millions of Tor users were
22 rendered highly vulnerable to attack by malicious third parties. According to a Twitter
23 statement released by Mozilla’s lead security expert, “[i]f this exploit was in fact
24 developed and deployed by a government agency, the fact that it has been published
25 and can now be used by anyone to attack Firefox users is a clear demonstration of how
26 supposedly limited government hacking can become a threat to the broader web.”

1 If part or all of the Operation Pacifier NIT components have been obtained by
2 Mozilla, or otherwise made available to the public, the Government's reliance on the
3 Classified Information Procedures Act and refusal to provide the defense with copies of
4 the code based on national security and law enforcement exemptions will need to be
5 reconsidered by the Court. *See* Local Cr. 12(b)(10)(A) (motions for reconsideration are
6 appropriate when based upon "new facts. . . which could not have been brought to [the
7 court's] attention earlier with reasonable diligence.").

8 Accordingly, the defendants request that the Court order the Government to
9 disclose whether the vulnerability that was patched by Mozilla on or about November
10 29, 2016, is related to the NIT code at issue in these cases.

11 In addition, if the patch and code are related, the Government should be required
12 to disclose the date on which it (or a contractor or agent for the Government) learned
13 that the NIT code had been published or otherwise made available to parties other than
14 the FBI.

15 The defendants also request a substitute summary of the evidence that was
16 presented to the Court *ex parte* in connection with the Government's CIPA and law
17 enforcement exemption claims.

18 The defense has no objection to the Court's issuance of a protective order in
19 connection with these disclosures.

20 ///

21 ///

22 ///

23 ///

24 ///

25 ///

26 ///

III. CONCLUSION

For the reasons stated above, the defendants respectfully request that Court order the Government to disclose the information sought by this motion.

DATED this 7th day of December, 2016.

Respectfully submitted,

s/ Colin Fieman

Attorney for David Tippens

s/ Robert Goldsmith

Attorney for Gerald Lesan

s/ Mohammad Hamoudi

Attorney for Bruce Lorente

CERTIFICATE OF SERVICE

I hereby certify that on December 7, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered with the CM/ECF system.

s/ Amy Strickling, Paralegal
Federal Public Defender Office